Security Requirements
(Loan Purchase Program)

Federal Student Aid agrees with the Office of Management and Budget (OMB) and Congress that the security of its data and IT resources is one of our highest priorities. Recognizing the need for agencies to have effective information security programs, Congress passed the Federal Information Security Management Act (FISMA) of 2002. FISMA provides the overall framework for ensuring the effectiveness of information security controls that support federal computer operations and assets. **FISMA requirements apply to all federal contractors and organizations or sources that possess or use federal information or that operate, use, or have access to federal information systems on behalf of an agency**. FISMA mandates the use of the standards created by the National Institute of Standards and Technology (NIST). and Federal Student Aid has adopted those standards and guidance for securing its information technology resources.

Federal Student Aid security requirements indicated below ensure the confidentiality, integrity and availability of its data at a high level. Additional detailed requirements can be found in NIST security standards, special publications, and bulletins; OMB memorandums; and the Department of Education (DoED) policies and procedures. The primary document Federal Student Aid uses to identify and implement controls is NIST SP 800-53.The latest version of this guidance can be found at http://csrc.nist.gov/publications/nistpubs/800-53-Rev2/sp800-53-rev2-final.pdf

Personnel

1. All personnel are required to complete a federal background clearance based on their position risk level. Background clearances are submitted on line via Office of Personnel Management (OPM)'s Electronic Questionnaire for Investigations Process (e-Qip). Contractor employees who have undergone appropriate personnel security screening for another federal agency may submit proof of personal security screening for validation. (Attached: Department of Education's Directive for *Contractor Employee Personnel Security Screenings*)
2. Preliminary clearances must be completed for high-risk positions prior to working on Federal Student Aid systems or data (This process can take 2-6 weeks). Moderate and low risk positions must submit background clearance paperwork prior to working on Federal Student Aid computer resources.
3. Non-U.S. Citizen may be assigned to a High Risk IT (6C) level position, provided: he/she is a Lawful Permanent Resident of the United States and has resided continuously in the United States for a minimum of three (3) years. Non-U.S. Citizens living outside of the United States cannot have the capability to access Federal Student Aid systems or data.

4. All personnel are required to successfully complete initial security awareness training within two weeks of employment and annual refresher training. The training can be completed on line using DoED’s security training program.
5. Annual specialized training is required that is appropriate to job function.

Facility

1. Data Centers supporting Federal Student Aid systems are required to have controlled access with working security cameras..
2. Data center access control lists must be kept current. .
3. Visitors must be logged and escorted at all times.
4. Power equipment and power cabling for the information system must be protected from damage and destruction. Facility failover power and lighting are required for emergencies.
5. The facility must employ and maintain fire suppression and detection, water damage controls, and temperature and humidity controls.
6. Alternate data center worksites are required to have the same protections as the primary data center site.

Telecommunications

1. Data transfers of PII or other sensitive information must be encrypted using NIST certified encryption methods (see NIST standard, FIPS 140-2)
2. All interconnections must be documented and have an Interconnection Security Agreement in place. (see NIST SP 800-47)
3. Wireless communication containing Federal Student Aid information is not permitted within the data center.
4. The Federal Student Aid System Security Officer must approve all remote access.

Contingency Planning and Recovery

1. A contingency / disaster recovery plan is required to provide continued operational service within 72 hours of a major catastrophe.
2. Contingency plans must be tested at a recovery site annually using both DoED and Contractor personnel.
3. The recovery site(s) must be geographically separated from the production site(s).
4. Data sanitation at the recovery site is required after testing. (see NIST SP 800-88)
5. System backups must be encrypted and kept at an alternate location with secured access. Sensitive backup tapes must be marked and have a secure transfer. (Attached: Federal Student Aid’s *General Support System and Major Application Backup Media Handling Policy & Procedures*)

Risk Management

1. Annual self-assessment of security controls is required. .
2. Independent risk assessments will be completed prior to system’s operation and then reassessed at a minimum of every three years.

3. Independent security controls assessment will be completed.
4. All identified vulnerabilities and security weaknesses will be captured and corrective actions tracked through Federal Student Aids Operational Vulnerability Management Solution (OVMS). Security remediations must be implemented to correct security deficiencies and appropriate evidence must be provided to close actions.
5. Contractors will make themselves and the site available for security audits and control assessments. This includes interviews with key security staff, data gathering and submissions, scanning support, and escort activities.
6. Federal Student Aid will have the right to test controls through independent scanning within the boundaries of the Federal Student Aid system and by other means like interviews, observations, and to document reviews.

Security Documentation

1. The contactor will develop and implement a system security plan (SSP) for the information system to provide an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within Federal Student Aid will review and approve the plan. (see NIST SP 800-18)
2. A contingency plan must be created, approved, and tested annually.
3. A configuration management plan must be created, approved, and implemented.
4. Documented system boundaries are required. A documented inventory of hardware and software utilized, telecommunication interconnections and a network topology are required. (Attached: Federal Student Aid's Boundary Definition template).
5. System access authorizations and signed rules of behavior must be maintained.
6. Plans of Actions and Milestones that address security remediations are maintained in Federal Student Aid's Operational Vulnerability Management Solution.

Security Monitoring and Detection

1. Network intrusion detection systems (NIDS) and host-based intrusion detection systems (HIDS) are configured appropriately and continuously monitored and updated if necessary.
2. Systems will have appropriate auditing capabilities enabled.
3. System logs are to be analyzed for suspicious activity. Logs will be made available to Federal Student Aid upon request.
4. Compliance monitoring established for configuration settings.
5. Routine network and database scans are scheduled. The scan results are analyzed and vulnerabilities identified. The identified vulnerabilities and actions taken will be documented in OVMS.
6. Scans that identify web vulnerabilities will be completed. Scan results will be provided to FSA upon request. The identified vulnerabilities and actions taken will be documented in OVMS.

7. Security remediations must be implemented to correct security deficiencies and appropriate evidence must be provided to close actions.

Incident Response

1. Contractor must maintain an incident response plan that correlates to the DoED plan.
2. Compromises of personal identifiable information (PII) must be reported immediately so that the Department can comply with its reporting requirements to report to U.S. Computer Emergency Readiness Team (CERT) within one hour of the incident.
3. Contractor must preserve evidence and allow external forensic analysis either on-site or through shipment of components.
4. Contractor must take appropriate actions for alerts and warnings provided by DoED or through other sources. Contractor will report status of their actions as requested.

Security Configurations

1. Federal Student Aid data must be segregated from non-Federal Student Aid data.
2. Security patches must be kept current and appropriately tested prior to moving into production.
3. Server and device security configurations must be maintained in accordance with NIST security configuration standards (See: http://checklists.nist.gov/).
4. Passwords must meet Federal Student Aid's password standards. (Attached: Federal Student Aid's *Password Parameters Policy & Procedures*)
5. Change control management procedures must be documented and followed.
6. Federal Student Aid must approve system changes prior to production implementation.
7. Data will be safeguarded commensurate with the highest categorization level based on FIPS 199.

Access Control

1. Federal Student Aid must approve all access to Federal Student Aid data and all contractor access that can affect any component within the system's boundary.
2. Application access reports need to be sent quarterly to Federal Student Aid for certification of access.
3. A listing of IT personnel responsible for operations and maintenance of any Federal Student Aid system must be provided on a quarterly basis to FSA for certification of access.
4. Access must be restricted based on least privilege. Role based access controls should be defined and documented.